Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A method of providing automated document retention for an electronic document comprising:

assigning a document retention policy to the electronic document, the document retention policy being derived from a recurring cut-off retention schedule specifying cut-off periods, each cut-off period having a respective ~~finite~~ document retention duration associated therewith and corresponding to a respective maximum off-line period of a client, wherein the maximum off-line period expires a predetermined period of time after a beginning of its cut-off period; and

encrypting the electronic document based on the document retention policy such that the electronic document can be cryptographically accessed only during ~~finite~~ retention durations and prior to the expiration of the maximum off-line period of the client.

2. (Currently amended) The method as recited in claim 1, wherein the encrypting the electronic document comprises encrypting using cryptographic keys associated with particular cut-off periods, ~~and~~ associated retention durations, and corresponding maximum off-line periods.

3. (Currently amended) The method as recited in claim 1, wherein

encrypting the electronic document comprises encrypting using a cryptographic key associated with each particular cut-off period, ~~and~~ its associated retention duration, and its corresponding maximum off-line period.

4. (Previously Presented) The method as recited in claim 3, wherein the document retention policy specifies the respective document retention duration that expires a predetermined period of time after a beginning of its respective cut-off period.

5. (Canceled)

6. (Previously Presented) The method as recited in claim 1, wherein said encrypting comprises acquiring a cryptographic key from a server over a network, the cryptographic key being used to encrypt the electronic document based on the document retention policy.

7. (Previously Presented) The method as recited in claim 6, further comprising:

deactivating the cryptographic key when the respective document retention duration has expired, thereby preventing further access to the electronic document.

8. (Previously Presented) The method as recited in claim 7, wherein:

said encrypting uses a cryptographic key to encrypt the electronic document based on the document retention policy, and

the document retention policy specifies respective document retention durations and cut-off periods.

9. (Previously Presented) The method as recited in claim 8, wherein the document retention policy specifies the respective document retention duration that expires a predetermined period of time after a beginning of its respective cut-off period.

10. (Currently amended) A method of limiting access to an electronic document comprising:

determining whether a cut-off period for a first document retention key has elapsed;

generating a next document retention key to be used to encrypt the electronic document during a next cut-off period, the next document retention key having a ~~finite~~ document retention duration associated therewith and corresponding to a maximum off-line period of a client, wherein the maximum off-line period expires a predetermined period of time after a beginning of the next cut-off period; and

notifying [[a]]the client of the next document retention key, the electronic document being cryptographically accessible only during ~~finite~~ document retention durations and prior to the expiration of the maximum off-line period of the client using a cryptographic key associated with such durations.

11. (Previously Presented) The method as recited in claim 10, further comprising:

deactivating a cryptographic key according to a predetermined schedule.

12. (Previously Presented) The method as recited in claim 11, wherein the document retention duration is a predetermined duration of time following a beginning of the next cut-off period.

13. (Currently amended) A method for restricting access to an electronic document, said method comprising:

encrypting a data portion of the electronic document using a document key to produce an encrypted data portion;

using a retention access key to associate a document retention policy with the electronic document;

encrypting the document key using the retention access key to produce an encrypted document key, the retention access key being usable for said encrypting during a cut-off period of a recurring cut-off retention schedule, the cut-off period having a ~~finite~~ document retention duration associated therewith and corresponding to a maximum off-line period of a client, wherein the maximum off-line period expires a predetermined period of time after a beginning of the cut-off period;

forming a secured electronic document from at least the encrypted data portion and the encrypted document key; and

storing the secured electronic document, the secured electronic document being cryptographically accessible only during the ~~finite~~ document retention duration and prior to the expiration of the maximum off-line period of the client.

14. (Previously Presented) The method as recited in claim 13, wherein the retention access key is a public retention access key.

15. (Previously Presented) The method as recited in claim 13, wherein the document retention policy specifies the document retention duration that expires a predetermined period of time after a beginning of its cut-off period.

16. (Currently amended) A method for accessing a secured electronic document, the secured electronic document having at least a header portion and a data portion, comprising:

obtaining a retention access key, the retention access key being used to associate a ~~finite~~ document retention duration of a document retention policy having a cut-off period and a maximum off-line period of a client associated therewith with the secured electronic document, wherein the maximum off-line period expires a predetermined period of time after a beginning of the cut-off period, the retention access key being usable during the document retention duration following a beginning of its respective cut-off period of a recurring cut-off retention schedule, the secured electronic document being cryptographically accessible only during the ~~finite~~ document retention duration and prior to the expiration of the maximum off-line period of the client;

obtaining an encrypted document key from the header portion of the secured electronic document;

decrypting the encrypted document key using the retention access key to produce a document key; and

decrypting an encrypted data portion of the secured electronic document using the document key to produce a data portion.

17. (Previously Presented) The method as recited in claim 16, wherein the retention access key is identified by an indicator within a header portion of the secured electronic document.

18. (Previously Presented) The method as recited in claim 16, wherein the retention access key is a private retention access key.

19. (Previously Presented) The method as recited in claim 16, wherein said obtaining obtains the retention access key from a server.

20. (Previously Presented) The method as recited in claim 16, wherein the document retention duration is a predetermined period of time following a beginning of its respective cut-off period.

21. (Currently amended) A tangible computer-readable medium having stored thereon, computer-executable instructions that, if executed by a computing device, cause the computing device to perform a method comprising:

assigning a document retention policy to an electronic document, the document retention policy being derived from a recurring cut-off retention schedule specifying cut-off periods, each cut-off period having a respective ~~finite~~ document retention duration associated therewith and corresponding to a respective maximum off-line period of a client, wherein the maximum off-line period expires a predetermined period of time after a beginning of its cut-off period; and

encrypting the electronic document based on the document retention policy such that the electronic document can be cryptographically accessed only during ~~finite~~ retention durations and prior to the expiration of the maximum off-line period of the client.

22. (Currently amended) The tangible computer-readable medium as recited in claim 21, wherein the encrypting the electric document comprises using cryptographic keys associated with particular cut-off periods, ~~and~~ associated retention durations, and corresponding maximum off-line periods.

23. (Currently amended) The tangible computer-readable medium as recited in claim 21, wherein the encrypting the electric document comprises using a cryptographic key associated with particular cut-off period, ~~and~~ its associated retention duration, and its corresponding maximum off-line period.

24. (Previously Presented) The tangible computer-readable medium as recited in claim 23, wherein the document retention policy specifies the respective

document retention duration that expires a predetermined period of time after a beginning of its respective cut-off period.

25. (Currently amended) A computer-implemented file security system for restricting access to an electronic file, comprising:

a module which if executed by a computing device of the computer-implemented file security system, causes the computing device to ~~computer-readable storage medium configured to~~ store a plurality of cryptographic key pairs on a computer-readable storage medium, each of the cryptographic key pairs including a public key and a private key, at least one of the cryptographic key pairs pertaining to a retention policy, the retention policy having ~~finite~~ document retention durations, each ~~finite~~ document retention duration having a respective cut off period associated therewith and corresponding to a respective maximum off-line period of a client, wherein the maximum off-line period expires a predetermined period of time after a beginning of its cut-off period; and

an access control management module which if executed by a computing device of the computer-implemented file security system, causes the computing device to:

provide, for each particular cut-off period, a different one of the public keys of the at least one of the cryptographic key pairs, and

determine whether the private key of the at least one of the cryptographic key pairs pertaining to the retention policy is permitted to be provided to a requestor based on whether its respective document retention duration following a beginning of its respective cut-off period has expired,

wherein the requestor requires the private key of the at least one of the cryptographic key pairs pertaining to the retention policy to access a secured electronic file, and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy, and at the time the electronic file was secured, the public key was within its respective cut-off period and available for use, the secured electronic document being cryptographically accessible only during the ~~finite~~ retention durations and prior to the expiration of the maximum off-line period of the client.

26. (Previously Presented) The method as recited in claim 13, wherein access is restricted to the secured electronic document stored to a remote location.